

**IN THE UNITED STATES DISTRICT COURT**  
**FOR THE DISTRICT OF COLUMBIA**

<b>IN THE MATTER OF THE SEARCH OF:</b>	)	<b>UNDER SEAL</b>
<b>A residential condominium located at</b>	)	
<b>The Watergate, 2700 Virginia Ave., N.W., #901</b>	)	<b>Case No.</b>
<b>Washington, D.C. 20037</b>	)	

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR SEARCH WARRANT**

I, Grayden R. Ridd, having been duly sworn, depose and state as follows:

**INTRODUCTION**

1. I make this affidavit in support of an application for a search warrant to search a residential condominium dwelling located at The Watergate, 2700 Virginia Avenue, N.W., #901, Washington, D.C. 20037. As set forth herein, there is probable cause to believe that at this location, there exists evidence, fruits, and instrumentalities of, and property intended for use in committing, violations of Title 50, United States Code, Sections 1701-1706 (International Emergency Economic Powers Act/Sudanese Sanctions Regulations), and Title 18, United States Code, Sections 951 (Agents of a foreign government) and 371 (Conspiracy).

**AGENT BACKGROUND**

2. I am a Special Agent of the Federal Bureau of Investigation ("FBI") and have served in that capacity since February 2009. I currently am assigned to the Counterintelligence Division of the FBI's Washington Field Office. As such, I am an "investigative or law enforcement officer" of the United States within the meaning of Title 18, United States Code, Section 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations of and to make arrests for offenses enumerated in Title 18, United States Code, Section 2516(1).

3. In the course of my duties, I am responsible for investigating violations involving espionage, acting as an illegal agent of a foreign power, United States trade sanctions, unauthorized retention and disclosure of classified and national defense information, money laundering in furtherance of national security offenses, and conspiracy to commit the said offenses. I have been working in this capacity since 2009. During my employment with the FBI, I have received specialized training in and employed the use of various investigative techniques, which include, but are not limited to, physical surveillance, search warrants, pen registers, trap and trace devices, wire taps, tracking devices, confidential sources, and audio and video recording devices. I have also received training and acquired experience concerning methods of operation used by persons involved in criminal activity and their efforts to cloak the identity of parties to the criminal activity or the nature of their involvement in the criminal activity. These methods often include steps to mask the source or nature of communications and financial transactions. Prior to my employment with the FBI, I worked in separate instances as a consultant and an attorney.

**SOURCE OF INFORMATION CONTAINED HEREIN**

4. The facts set forth in this affidavit are based upon my personal knowledge, training and experience, personal involvement in this investigation, interviews conducted during the course of this investigation, information conveyed to me by other law enforcement officials, and my review of records, documents and other physical evidence obtained during this investigation.

5. I have not set forth each and every fact learned during the course of this investigation. Rather, I have set forth only the facts that I believe are necessary to establish probable cause for the issuance of a search and seizure warrant based on the instant affidavit.

## **EXPORT LAWS AND REGULATIONS**

### **International Emergency Economic Powers Act and the Sudanese Sanction Regulations**

6. The Republic of Sudan is a country located in northeast Africa. Its capital is Khartoum. Sudan has been in virtually continuous internal conflict since becoming independent in 1956, resulting in the deaths of hundreds of thousands of people and the displacement of millions. As a result of the Sudanese government's complicity in this conflict, the United States has imposed sanctions against Sudan since 1997. The International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C. §§ 1701-1706, authorizes the president of the United States to impose economic sanctions on a foreign country in response to an unusual or extraordinary threat to the national security, foreign policy, or economy of the United States, when the President declares a national emergency with respect to that threat.

7. On November 3, 1997, the President issued Executive Order ("E.O.") 13067, finding that "the policies and actions of the Government of Sudan, including continued support for international terrorism; ongoing efforts to destabilize neighboring governments; and the prevalence of human rights violations, including slavery and the denial of religious freedom, constitute an unusual and extraordinary threat to the national security and foreign policy of the United States," and declaring a national emergency, by Presidential Notice each year through to the present.

8. E.O. 13067 imposed a comprehensive trade embargo against Sudan and a total asset freeze against the Government of Sudan. Among other things, E.O. 13067 prohibited:

"the exportation or reexportation, directly or indirectly, to Sudan of any goods, technology . . . or services from the United States or by a United States person, wherever located, or requiring the issuance of a license by a Federal agency" [except for certain humanitarian donations];

“the facilitation by a United States person, including but not limited to brokering activities, or the exportation or reexportation of goods, technology, or services . . . to Sudan from any location”;

“the performance by any United States person of any contract . . . in support of an industrial, commercial, public utility, or governmental project in Sudan”; and

“[a]ny transaction by any United States person or within the United States that evades or avoids, or has purpose of evading or avoiding, or attempts to violate, any prohibitions set forth” in E.O. 13067.

9. To implement Executive Order 13067, the Secretary of the Treasury promulgated the Sudanese Sanctions Regulations, 31 C.F.R. part 538. The United States Department of the Treasury’s Office of Foreign Assets Control (“OFAC”), located in the District of Columbia, was and is the entity empowered to authorize transactions with Sudan. Such authorization, if granted, would be in the form of a license. Under the Sudanese Sanctions Regulations, it was and is a crime for any United States person to willfully engage in any transaction with the Government of Sudan without having first obtained a license or other authorization from OFAC.

10. On October 13, 2006, the President issued Executive Order 13412, adding to and clarifying the prohibitions set forth in E.O. 13067 by, among other things, specifically prohibiting “all transactions by United States persons relating to the petroleum or petrochemical industries in Sudan, including, but not limited to, oilfield services and oil or gas pipelines.” E.O. 13412 lifted the prohibitions of E.O. 13067 for certain regions of Sudan including Southern Sudan and Darfur, so long as the activities and transactions there “do not involve any property or interests in property of the Government of Sudan.” E.O. 13412 also prohibited “any transaction by any United States person or within the United States that evades or avoids, or has the purpose

of evading or avoiding, or attempts to violate, any prohibition set forth” in E.O. 13412, as well as any conspiracy formed to violate any of its prohibitions.

11. IEEPA provides criminal penalties for willful violations of its restrictions, including the restrictions imposed by the Sudanese Sanctions Regulations.

12. Furthermore, Title 18, United States Code, Section 951(a) provides criminal penalties for any person who, “other than a diplomatic or consular officer or attaché, acts in the United States as an agent of a foreign government” without providing notice as such with the Foreign Agent Registration Act Unit (FARA Unit) of the United States Department of Justice. An “agent of a foreign government” includes a person “who agrees to operate within the United States subject to the direction or control of a foreign government or official.” 18 U.S.C. § 951(d). It is a crime for such a person to engage within the United States in an otherwise legal commercial transaction, if the person is acting subject to the direction and control of a foreign government or official of a country that the President has determined (and so reported to Congress) is a threat to the national security of the United States for the purpose of the statute. 18 U.S.C. § 951(e).

### **FACTS SUPPORTING PROBABLE CAUSE**

#### **Report of Criminal Conduct**

13. On September 30, 2009, it was reported in the *Washington Post* that Robert McFarlane, a former national security advisor, was hired by the government of Sudan to lobby the United States on its behalf. The article stated with particularity that Robert McFarlane was approached in late 2008 by Sudanese officials, to include members of the Sudanese intelligence service, in an effort to enlist his aid in gaining access to the new administration in Washington, D.C. for the purpose of persuading it to lift sanctions and to remove Sudan from a list of state

sponsors of terrorism. It was reported that the Sudanese strategy, which they dubbed “Plan Tragacanth,” ultimately led to a \$1.3 million contract.

14. The author of the article stated that through “internal e-mails and other documents obtained by *The Washington Post*,” he was able to determine details concerning the contract. Specifically, it was reported that a Sudanese diplomat played a central role in proposing and securing a contract between McFarlane and the country of Qatar, and that Sudanese officials discussed the need to provide McFarlane and others funds once the agreement was complete. The article reported that “McFarlane recounted in an e-mail, he was approached by a former business partner, Albino Aboug, on behalf of Sudan’s government;” and that in early January 2009, McFarlane met with Aboug and Sudanese official Mohammed Babiker in Dubai, United Arab Emirates, to discuss the contract. The article described a month-long exchange of e-mails between McFarlane and Babiker in January 2009, culminating with McFarlane’s contract with Qatar. The article included scanned images of several e-mails, all dated January 2009, between McFarlane and Babiker, in which it partially identified McFarlane and Babiker’s e-mail accounts and included some of the above-described substance. The article continued to state that it was agreed that McFarlane would represent the government of Sudan through the government of Qatar, which was to act as a third party to hide the direct connection between McFarlane and the government of Sudan.

15. According to the article, Sudanese officials asked McFarlane to approach four former U.S. diplomats to ask if they were interested in assisting their effort and a proposed budget of \$100,000 a month was set aside to pay them. The article reported that McFarlane approached the four former diplomats and was turned down. The article identified three of the former diplomats and offered quotes in which they acknowledged that they were approached by McFarlane and stated that they did not accept his offer.

16. The article also stated that McFarlane e-mailed a copy of the proposed contract with Qatar to Babiker ““for your consideration”” before it was signed. It was reported that the final contract was signed on February 9, 2009, in Doha, Qatar’s capital, with Sudanese officials present. The article further reported that according to a fee schedule sent from McFarlane to Babiker, he was to receive a salary of \$410,400.

Corroboration

A. Cooperating Witness

17. On March 16, 2010, the FBI interviewed a Cooperating Witness (CW). The CW advised that, as part of his relationship with a citizen of Sudan, he was familiar with McFarlane’s contract with Qatar. The CW advised that while the contract was with Qatar, McFarlane was actually working for the Sudanese government, and that the work included lobbying officials within the United States government on behalf of the government of Sudan. The CW provided the FBI several documents in support of its statement. These documents – which do in fact support the CW’s statement – appear to be internal e-mail communication and memoranda dated January 2009 through February 2009 related to McFarlane’s contract. I have highlighted the most significant documents.

18. All of the below described e-mails involve communication between or concerning McFarlane and officials within the government of Sudan. The source of the e-mails appears to be someone within the Sudanese intelligence service. I say this because all of the e-mails have been forwarded from “Mohammed” at e-mail account [mhbabiker@peacesudan.org](mailto:mhbabiker@peacesudan.org) (Mohammed Babiker’s e-mail account”) to “Khalid Yousif” at [nisshq@yahoo.com](mailto:nisshq@yahoo.com) (“NISS e-mail account”). I believe “Mohammed” is Mohammed Hassan Babiker (“Babiker”), a Sudanese government official. Open source reporting lists Babiker as a Sudanese diplomat associated with the Sudanese embassy in Addis Ababa, Ethiopia. The CW reported to me that Babiker is actually an

operative of the Sudanese intelligence service, which I know to be the National Intelligence and Security Service (“NISS”). I also know from other investigations that the e-mail header “nisshq” is used by the NISS.

19. In a string of emails, dated January 14, 2009 through January 16, 2009, between Babiker’s e-mail account and “Robert McFarlane” at [rcm@mcfarlaneassociateinc.com](mailto:rcm@mcfarlaneassociateinc.com), Babiker referenced a meeting a week earlier in Dubai and sent McFarlane an article concerning Senator Hillary Clinton’s testimony about Sudan before the Senate during her confirmation hearings as Secretary of State. McFarlane acknowledged that he had seen the testimony and stated that he thought it “unwise to be so categorical and critical before engaging in preliminary talks.” McFarlane went on to say he discussed Sudan with two former U.S. government officials and they were interested in “working on this agenda.” McFarlane stated that he was going to approach a third former U.S. government official. Babiker acknowledged that “the noble mission you are striving to work is not an easy task” and stated that “I’m quite confident that you and the other gentlemen in your team will be capable to convince the Administration with realities.” Babiker noted that the “gentlemen [McFarlane] had talked to know Sudan well.” Babiker also advised that “Mr. Albino worked very hard to obtain a license and that a high level delegation in Qatar [agreed] to discuss about third party sponsorship.” On January 20, 2009, these e-mails were forwarded from Babiker’s e-mail account to the NISS e-mail account. I believe that this is a discussion about steps McFarlane has taken and plans to take in assembling a team with which to provide advice to Sudan and to lobby the U.S. government on behalf of Sudan. I also believe that Babiker’s reference to Albino and Qatar suggests that Albino Aboug<sup>1</sup>

---

<sup>1</sup> Albino Aboug is often referred to as “Albino” or “Aboug.” I have tried to use the name exactly as it appears in the underlying source document. Therefore, for purpose of this affidavit, the names are used interchangeably.



has some involvement in securing the government of Qatar to act as a sponsor for the McFarlane–Sudan agreement.

20. In a string of emails, dated January 24, 2009 through February 2, 2009, between Babiker’s e-mail account and Robert McFarlane at his e-mail account, McFarlane stated that he had spoken “with the four gentlemen who were involved in the negotiation of the CPA<sup>2</sup> and whom your delegation leader characterized as trustworthy.” McFarlane advised that he asked for their views as well as their “personal interest in participating in an advisory effort directed toward peace.” McFarlane went on to state this will ultimately require government-to-government involvement, but “before proceeding we should engage privately with the relevant cabinet-level officials.” Babiker then advised that this was a good move and that “[w]e are really counting on your wisdom.” He stated that he had “received the draft agreement of the third party from Mr. Albino.” McFarlane then explained that he did not have a business relationship with Albino but was “open to an arrangement through Albino or directly.”

21. Babiker then stated that “we prefer to have the direct link with you so we can do any arrangement necessary for this kind of work directly.” Babiker stated that Albino “gave [him the] draft agreement to be signed by [McFarlane] with the third party (Qatar).” McFarlane then went on to describe his relationship with Albino. He stated that they met in Khartoum in 2007, at which time Albino asked McFarlane if he was interested in advising the government of Southern Sudan on how to attract investment and stimulate growth in its economy. McFarlane stated that he agreed to provide such consulting services in July 2008 and established a U.S. company – U.S.–Southern Sudan Development Company – to carry out the work. He said the agreement expired on December 31, 2008.

---

2 I believe that the “CPA” stands for the Comprehensive Peace Agreement, which was signed on January 9, 2005 by the government of Sudan and the former southern rebels of the Sudan People’s Liberation Movement/Army. The United States played a significant role in brokering this agreement.

22. McFarlane continued that he was approached by Albino in November 2008 and asked if would be willing to discuss with senior representative from the Khartoum government how to foster the peace process and renewed diplomatic relations. McFarlane stated that this “led to our meeting in Dubai,” at which time Sudanese officials provided the names of “trustworthy” former U.S. officials who might be “willing to provide informal counsel.” McFarlane stated that he preferred that the agreement “be through a third party with established auspices over the Darfur peace process.” McFarlane again acknowledged that he had approached the former U.S. government officials and that he “found them open to participating in this effort.” McFarlane stated that at Albino’s request, he drafted an agreement which could be offered “to the Government of the third country . . . but I stressed to him that I (and I believe any former official) would want a more direct channel to the ‘client.’” McFarlane stated that he transferred his interest in the U.S. company to Albino. McFarlane ended by saying that he and his “colleagues are ready to proceed as we discussed in Dubai and will await further word from your side as to the best approach.” Babiker thanked McFarlane and restated issues that needed to be addressed with the administration, which included:

- “1. Peace in Darfur, including the ICC threat to peace.<sup>3</sup>
2. Bilateral relations; including sanctions, terror list, and development issues.
3. Peace and unity of Sudan: the role of the US government in fostering unity of the country.”

23. Babiker asked McFarlane to draft an “action plan for the way forward.” McFarlane thanked Babiker and asked if Babiker could “advise the third country that [McFarlane] would be pleased to submit a proposal . . . and could be available to sign it on any

---

<sup>3</sup> I believe that the “ICC” stands for the International Criminal Court, which indicted Sudan’s president, Omar Hassan Ahmad al-Bashir, for war crimes and crimes against humanity. An arrest warrant was issued by the ICC for al-Bashir’s arrest on March 4, 2009.

day except February 14<sup>th</sup>.” Babiker again thanked McFarlane and stated that “we have discussed this issue with the Qatari government and they accepted to sponsor.” Babiker stated that they wanted to meet in Doha on February 9, 2009 to sign the agreement. McFarlane stated that he would be available to sign the agreement in Doha on the suggested date. He also reemphasized that he was willing to “engage in this effort either as a subcontractor to Albino’s company or directly.” A document titled, “GOQ Agreement 2-2-09” was attached to this latest McFarlane e-mail.

24. On February 2, 2009, these e-mails were forwarded from Babiker’s e-mail account to the NISS e-mail account. I believe that these e-mails are evidence that McFarlane was entering into an agreement with the government of Sudan to lobby the U.S. government officials on behalf of Sudan and to provide it advice during negotiations with the United States. It is further evidence of an attempt by McFarlane and Babiker to hide McFarlane’s relationship with Sudan by construing the agreement to make it appear that his contractual relationship was with Qatar, when in fact it was not.

25. In an e-mail, dated February 4, 2009, from Robert McFarlane at McFarlane’s e-mail account to Babiker’s e-mail account, McFarlane asked Babiker to have the government of Qatar forward McFarlane a letter of invitation to come to Doha to discuss reconciliation in Sudan. McFarlane provided Babiker the proposed text of the letter of invitation. On February 5, 2009, this e-mail was forwarded from Babiker’s e-mail account to the NISS e-mail account. Babiker advised “Khalid” that McFarlane needed an “invitation from the host to avoid any inconvenience that he may face in the future” and asked him to pass along the draft letter.

26. In addition to the above described e-mails, the CW provided several documents which supported his statement. The documents include a draft contract, a projected budget, and several letters in Arabic. The contract is titled, “Agreement By and Between McFarlane

Associates, Inc. and the Government of Qatar.” According to the terms of the contract, McFarlane Associates Inc. (MAI) was to provide services to Qatar which included: (1) assistance in its effort to “broker peaceful settlements between the Government of Sudan in Khartoum and the people of Darfur to include securing the assistance of respected U.S. third-parties towards this objective” and (2) to assist it “in facilitating additional agreements between the Government of Sudan in Khartoum and all marginalized ethnic groups in Sudan and to secure the assistance of respected U.S. third-parties towards this objective.” The agreement states that term of the agreement will run from February 9, 2009 through February 8, 2010 and that “compensation will be in accordance with the enclosed budget.” The agreement also stated that it could be extended upon the mutual consent of the parties. A document, titled “Projected Budget 2009,” provides for a projected annual budget of \$2,473,650. It includes, among other expenses, a monthly retainer for MAI in the amount of \$63,500, and a monthly allotment for four advisors in the amount of \$100,000. The CW stated that he believed that these two documents were forwarded by McFarlane to Babiker as an attachment to one of the above described e-mails.

27. The CW also provided several letters, which were in Arabic text.<sup>4</sup> Translations of these documents reveal that they are letters from “Mohammad Hassan Babiker, Official of Addis Abada” and addressed to “Mr. Director General.” In a letter, dated January 14, 2009, Babiker proposed the code name, “Plan Tragacanth,” for the “special work to attempt to communicate with the new American administration and improve the image of Sudan against the American and Western deceptions about Sudan.” It is also apparent from this letter and a similar letter, dated January 19, 2009, that Babiker utilized code names when referring to Albino Aboug and McFarlane, whom he called “Rambo” and the “Ordained,” respectively. In the January 19, 2009 letter, Babiker provided an update on McFarlane’s efforts on behalf of Sudan; specifically, that

---

<sup>4</sup> I would note that Arabic and English are the official languages of Sudan.

McFarlane had spoken with former U.S. officials and would continue to speak with other individuals. Babiker stated that he sent the “Ordained” Hillary Clinton’s testimony and included McFarlane’s comments about the testimony. Babiker stated that he received the above described agreement with Qatar from “Rambo” and that they (Albino and McFarlane) wanted the Sudanese to review it and state any concerns before it was signed. Babiker included with the letter, the draft contract and an e-mail, dated January 16, 2009, from “Robert C. McFarlane” at McFarlane’s e-mail account to “Albino” at [ayuel@netzero.net](mailto:ayuel@netzero.net), in which McFarlane stated that it sounded like Albino was making progress in Doha. McFarlane also identified several former U.S. officials as potential team members that were recommended by Salah Gosh.<sup>5</sup>

28. Finally, in a letter dated January 25, 2009, Babiker relayed that the “Ordained” (McFarlane) summarized his recent efforts to assist Sudan, which included getting several former U.S. officials to assist in an advisory capacity. Babiker noted that the “ordained is striving to achieve this breakthrough and is focused on helping us first and foremost.” Babiker recommended supporting “the agreement of the three sides” and “then provid[ing] the necessary money for the activities of the group.” I believe that these letters represent Babiker reporting to Salah Gosh or another high level minister within the government of Sudan McFarlane’s efforts on behalf of Sudan and the steps taken to secure a contract with McFarlane through a Qatar, which is acting merely as a third party sponsor.

B. Further Investigation of Unlawful Foreign Agent Status

29. The FBI investigation revealed that Robert McFarlane is a U.S. person and that he does not nor has he ever possessed an OFAC license to represent the government of Sudan, or has he otherwise been so authorized by the United States government. He is therefore barred by the Sudanese Sanctions Regulations from providing any services to the government of Sudan –

---

<sup>5</sup> I know from prior investigations and open source reporting that in January 2009 and continuing through June 2009, Salah Gosh served as the Director General of the Sudanese NISS.

to include lobbying the United States government on behalf of the government of Sudan. The investigation also revealed that McFarlane served as the chairman of MAI, a small consulting firm located in Arlington, Virginia, until approximately late April, 2011.

30. According to U.S. Department of Justice records, on November 9, 2009, MAI submitted a registration package to its FARA Unit, in which MAI acknowledged a contract with the government of Qatar, with the admitted purpose of participating in the peace process in Sudan. MAI indicated that it would not be engaged in political activities, in the course of the execution of the contract. MAI declared a total of four agents of a foreign principal, including McFarlane (whom is identified as the chairman of MAI), Amanda K. Jane and Catherine E. Neuner. MAI indicated that its services for the government of Qatar began in May 2009. Attached to the FARA registration package is a contract, signed by McFarlane and dated May 9, 2009, and a proposed budget. These two documents appear to be the same documents that McFarlane forwarded to Babiker in January 2009 as an e-mail attachment.

31. The FBI investigation has established significant contact between McFarlane and Albino Aboug, suggesting a business relationship related to Sudan. According to travel records obtained by the FBI, McFarlane and Aboug were both in Sudan in April 2007. Corporate records establish that shortly thereafter, on July 17, 2008, Aboug registered the U.S.- Southern Sudan Development Company (U.S.-SSDC) in the state of Colorado. Travel records indicate another meeting between McFarlane and Aboug. They both traveled to Alaska in mid-August 2008, and their airfare was purchased with the same credit card. Banking records show that a financial relationship ensued shortly after this meeting. Specifically, the U.S.-SSDC made three wire transfers totaling \$300,000 to MAI or MAI associates – (1) on September 30, 2008, U.S.-SSDC made a \$100,000 payment to MAI; (2) on that same date, U.S.-SSDC made a \$100,000 payment to Catherine Neuner; and (3) on October 1, 2008, U.S.-SSDC made a \$100,000

payment to MAI. Based, in part, on the explanation McFarlane gave Babiker about his relationship with Aboug, I believe these payments are for consulting services McFarlane and/ or MAI provided Sudan, possibly Southern Sudan, on economic growth.

32. A closer examination of U.S.-SSDC suggests that it is being used as a shell company. U.S.-SSDC is registered in Colorado; it, however, listed a Virginia address in the wire transfer paperwork. This Virginia address is the same address used by MAI. Also, on February 10, 2010, the FBI located a business card in the trash of MAI. The business card listed Catherine Neuner as the Vice President and CFO of “U.S. Southern Sudan Development Company.” It also listed a telephone number used by MAI. On March 1, 2010, I called the number on the business card, and the individual answered the phone, “McFarlane Associates.”

33. A past inspection of MAI’s trash established additional links between McFarlane and the government of Sudan and McFarlane’s use of his e-mail account to discuss Sudan related issues. On February 19, 2010, a handwritten note, dated “3/2,” was recovered from MAI’s trash. It was written on Sheraton, Doha, stationary and references “Salah Gosh” (the then Director General of the Sudanese intelligence service). It includes notes near his name about enemies of the government of Sudan within the United States, listing Save Darfur as an example (which is presumably the Save Darfur Coalition, an U.S.-based advocacy group calling for international intervention in Darfur). On the same page there is a reference to Khartoum’s goals and changing perceptions of “DoD, Dos, [and] Think Tanks” (likely meaning the U.S. Department of Defense and the U.S. Department of State). There is a notation about using a “PR firm,” and the name Amanda also appears on the note followed by “get suggestions from DoS.” Travel records obtained by the FBI show that McFarlane and MAI associate Amanda Jane traveled to Doha, Qatar in March 2009. These notes appear to have been taken during a March 2009 meeting with Sudanese officials shortly after the signing of the Qatar contract.

34. During the search of MAI's trash on February 19, 2010, the FBI located an e-mail, dated February 1, 2010, from Steve Kellar to McFarlane at McFarlane's e-mail account and Amanda Jane (at her MAI e-mail account), in which Kellar reported a meeting with Sudanese political figure Ahmed Deraige.<sup>6</sup> In the e-mail, Kellar stated that he told Deraige that he worked for McFarlane. Kellar stated that Deraige asked if McFarlane represented "State" (presumably the U.S. Department of State). Kellar stated that he told Deraige that McFarlane did not, but "had communications at the highest levels in the U.S. and elsewhere" and then "explained the Doha connection." This corroborates the claim made in the *Washington Post* article and by the CW that Qatar was simply acting as a third party to hide McFarlane's connection to the government of Sudan.

35. An undated outline, titled "US-Sudan Bilateral Relations," was located in MAI's trash on February 19, 2010. The outline contains lists of actions each government would like the other to take. Included in the list of items associated with Sudan are statements about allowing the government of Sudan to hire "US legal, lobbying and public relations assistance" and initiating action to remove Sudan from the list of State Sponsors of Terror. An undated agenda was also found in MAI's trash on February 19, 2009, along with the above referenced outline. The agenda, which contains several references to Sudan, references actions in the U.S. since the last meeting, including beginning an engagement with Congress and dialogue with State and Defense Departments; and launching several economic projects in Sudan, including a sugar plantation and a gas-capture and propane project.

36. On February 19, 2010, the FBI discovered an e-mail, dated February 10, 2010, about the travel of a Sudanese official. The e-mail was from a travel agency to Amanda Jane's MAI e-mail account. The e-mail includes an invoice and itinerary for Ahmed Abdolsofi, a

---

<sup>6</sup> I know that during this time period Ahmed Deraige was a Sudanese political leader representing the Darfur region of Sudan.



leader of a rebel group in Sudan. The invoice indicated that Abdolsofi was to stay at a hotel in Nairobi, Kenya on February 11, 2010, and then he was to fly from Nairobi to Entebbe, Uganda. Another invoice in McFarlane's name was found in MAI's trash on February 19, 2010. The invoice put McFarlane at the same Nairobi hotel on February 11, 2010. Travel records also indicated that the two trips were paid for by a credit card bearing the same last four digits (suggesting that they were paid for by the same credit card).

37. The FBI located additional evidence of McFarlane's travel to Sudan. On March 2, 2010, the FBI located an e-mail, dated September 9, 2009, from Robert McFarlane at McFarlane's e-mail account to a MAI employee, asking for itineraries to Khartoum for October 2009. An itinerary in McFarlane's name and dated September 10, 2009 was discovered on March 2, 2010, indicating McFarlane's travel to Khartoum in early October 2009.

38. On March 2, 2010, the FBI discovered an e-mail dated February 18, 2010 in MAI's trash. The e-mail is from McFarlane at McFarlane's e-mail account to several e-mails which appear from their names to be various think tanks in the United States, including the Nixon Center and the American Foreign Policy Council, and a member of the Senate Foreign Relations Committee. In the e-mail, McFarlane states that he has been working in the Darfur region and on issues related to U.S. oil independence. He then invites the recipients to get together for a meeting. I believe that this is evidence that McFarlane is following through earlier requests by the government of Sudan by contacting U.S. think tanks and U.S. government officials on their behalf.

39. Three additional items were located inside MAI's trash that suggest that McFarlane extended his contract with Qatar and thereby continued to provide services to the government of Sudan. On March 11, 2010, the FBI located a document titled, "MAI To DO List, Week of March 15-19, 2010." This document makes several references to Sudan and lists

steps to be undertaken, including “Draft Confidence Building Measure,” under which it lists “GOS Actions” (presumably the government of Sudan) and “US action.” The document identifies another step as “Public Affairs Plan,” in which it discusses, among other things, “Reciprocal Measures . . . by USG & GoS,” “Parallel Measures outside of governments (e.g. think tanks and media),” and references the importance of a water aquifer. On March 12, 2010, the FBI located a handwritten note that states, “Extension of GoQ contract.” I would note that the original contract with Qatar allowed for a six month extension upon the mutual consent of the parties. Moreover, on April 2, 2010, the FBI located a discarded e-mail, dated March 31, 2010, from McFarlane at McFarlane’s e-mail account to two of his associates at MAI (Amanda Jane and Catherine Neuner) regarding Sudan. Specifically, McFarlane discusses in the e-mail a meeting he had with a Sudanese government official and a suggested plan for proceeding in peace negotiations in Sudan.

40. On April 18, 2010, the FBI executed a search warrant on McFarlane’s email address, [rcm@mcfarlaneassociates.com](mailto:rcm@mcfarlaneassociates.com). In addition to corroborating the above narrative, the emails recovered in the April 18 search included emails directed to and sent from an additional Sudanese official, Yahia Babiker, at the email address [yahia.babiker@gmail.com](mailto:yahia.babiker@gmail.com) (the target email account). I know from open-source information that Yahia Babiker is a former deputy director of NISS, and that he currently serves as a special advisor to Sudanese President Omar Bashir. I also know, from other investigations, that Yahia Babiker has been involved in efforts to secure the services of U.S. persons to lobby or otherwise influence U.S. policy with regard to Sudan. Among the emails obtained via the April 18 search warrant was one sent from McFarlane’s email account to [yahia.babiker@gmail.com](mailto:yahia.babiker@gmail.com) and dated February 08, 2009. In it, McFarlane references having met with Yahia Babiker in Dubai a month earlier and lays out a plan by which he will assist the Government of Sudan in achieving its goal of “normalization of

relations.” McFarlane recalls that, in the Dubai meeting, it had been McFarlane’s suggestion to utilize a “sovereign third country,” and conduct the work through a “company with no affiliation to the government of Sudan (...for example my company McFarlane Associates Inc.).”

McFarlane also states “I believe that in proceeding as we’ve recommended above, we will be able to work together successfully.”

41. A Gmail response, dated June 20, 2012, to a 2703(d) Order showed a number of emails between [rcm@mcfarlaneassociates.com](mailto:rcm@mcfarlaneassociates.com) and [yahia.babiker@gmail.com](mailto:yahia.babiker@gmail.com), to include emails that were sent after the execution of the April 18, 2010 search warrant. Some of these emails are as recent as June of 2011.

42. On March 5, 2013, Robert McFarlane was interviewed by special agents of the FBI. In that interview, McFarlane stated he had closed his office in the spring of 2011 and that he now worked, when he worked, from home. The interviewing agents asked if he had transferred his documents and computers to his home as he established his home office, and McFarlane affirmed that he had.

43. In sum, the FBI investigation has established that in February 2009, McFarlane entered into a one year agreement with the government of Sudan to act as its consultant and to lobby the United States government on its behalf. McFarlane attempted to hide his relationship with Sudan by contracting with the country of Qatar, a third party “sponsor.” McFarlane used his e-mail account from at least January 2009 through March 2010 to, among other things: (1) negotiate an agreement with the government of Sudan; (2) discuss the services he was to provide or provided to the government of Sudan and payments he would receive for those service; (3) communicate with or take direction from government of Sudan officials; (4) communicate with, seek advice from, or lobby former or present U.S. officials on behalf of Sudan; and (5)

coordinate travel associated with performance of the services provided to or on behalf of the government of Sudan.

Items to be Seized

44. Based on my training and experience and the evidence uncovered in this investigation, I know that individuals involved in commercial and business transactions with prohibited countries, in violation of IEEPA, generally keep detailed business records. These business records, kept in either paper or electronic form, may include, but are not limited to, e-mail and other forms of correspondence, handwritten notes, meeting agendas, contracts, invoices, purchase orders, bank records, financial statements, ledgers, spreadsheets, travel records, and passports. In addition, I know that individuals who unlawfully operate in the United States as agents of a foreign government will employ various means to disguise the true nature of their work on behalf of the particular foreign government, including the use of third parties through which payments for services are made. Accordingly, such arrangements are typically documented through contractual agreements and written communications in either paper or electronic form.

45. The warrant application requests authorization to search for and seize all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any electrical, electronic, or magnetic form (such as any information on an electronic or magnetic storage device, including fixed hard drives, portable hard drives, thumb drives, floppy diskettes, CD-ROMs, DVD-ROMs, optical discs, backup tapes, printer buffers, smart cards, cellular phones, as well as printouts or readouts from any magnetic storage device (hereinafter collectively referred to as “digital devices”)); any handmade form (such as writing, drawing, painting); any mechanical form (such as printing or typing); and any photographic form (such as photocopies or digital photos).

46. In searching for digital devices and in searching digital data stored on digital devices, law enforcement personnel executing this search warrant will employ the following procedure:

a. Law enforcement personnel or other individuals assisting law enforcement personnel will, in their discretion, either search the digital device(s) on-site or seize and transport the device(s) to an appropriate law enforcement laboratory or similar facility to be searched at that location. The team of law enforcement personnel, which may include the investigating agent(s), and/or individuals assisting law enforcement personnel searching the digital device(s) shall complete the search as soon as is practicable but not to exceed 60 days from the date of execution of this warrant. If additional time is needed, the government may seek an extension of this time period from the Court within the original 60 day period from the date of execution of the warrant.

b. The team searching the digital devices will do so only by using search protocols specifically chosen to identify only the specific items to be seized under this warrant.

i. The team may subject all of the data contained in the digital device capable of containing items to be seized as specified in this warrant to the protocols to determine whether the digital device and any data falls within the items to be seized as set forth herein. The team searching the digital device may also search for and attempt to recover “deleted,” “hidden” or encrypted data to determine, pursuant to the protocols, whether the data falls within the list of items to be seized as set forth herein.

ii. The team searching the digital device also may use tools to exclude normal operating system files and standard third-party software that do not need to be searched.

c. When searching a digital device pursuant to the specific protocols selected, the team searching the digital device shall make and retain notes regarding how the search was conducted pursuant to the selected protocols.

d. If the team searching a digital device pursuant to the selected protocols encounters immediately apparent contraband or other evidence of a crime outside the scope of the items to be seized, the team shall immediately discontinue its search of that digital device pending further order of Court and shall make and retain notes detailing how the contraband or other evidence of a crime was encountered, including how it was immediately apparent contraband or evidence of a crime.

e. At the conclusion of the search of the digital devices as set forth in subparagraph (a) above, any digital device determined to be itself an instrumentality of the offense(s) and all the data thereon shall be retained by the government until further order of court or one year after the conclusion of the criminal case/investigation.

f. Notwithstanding the above, after the completion of the search of the digital devices as set forth in subparagraph (a) above, the government shall not access digital data falling outside the scope of the items to be seized in this warrant on any retained digital devices or digital data absent further order of court.

g. If the search team determines that a digital device is not an instrumentality of any offense under investigation and does not contain any data falling within the list of items to be seized pursuant to this warrant, the government will as soon as practicable return the digital device and delete or destroy all the forensic copies thereof.

h. If the search determines that the digital device or the forensic copy is not an instrumentality of the offense but does contain data falling within the list of the items to be seized pursuant to this warrant, the government either (i) within the time period authorized by the

Court for completing the search, return to the Court for an order authorizing retention of the digital device and forensic copy; or (ii) retain only a copy of the data found to fall within the list of the items to be seized pursuant to this warrant and return the digital device and delete or destroy all the forensic copies thereof.

47. In order to search for data that is capable of being read or interpreted by a digital device, law enforcement personnel are authorized to seize the following items, subject to the procedures set forth above:

- a. Any digital device capable of being used to commit, further or store evidence of the offenses listed above;
- b. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices and optical scanners;
- c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones and personal digital assistants;
- d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;
- e. Any applications, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;
- f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and
- g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.

48. The special procedures relating to digital devices and media found in this warrant govern only the search of digital devices and media pursuant to the authority conferred by this warrant and do not apply to any search of digital devices and media pursuant to any other court order.

**CONCLUSION**

49. Based upon the facts set forth in this Affidavit, and my training and experience as a law enforcement agent, I submit that there is probable cause to believe that evidence of violations of Title 50, United States Code, Sections 1701-1705 (International Emergency Economic Powers Act/Sudanese Sanctions Regulations); Title 18, United States Code, Sections 951 (Agents of a foreign government) and 371 (Conspiracy), will be found on the premises and digital devices located at or within 2700 Virginia Avenue NW, #901, Washington, D.C. Accordingly, I respectfully request that the Court issue a search warrant for the premises described in Attachment A, to include digital devices found within the premises, allowing agents to seize the information, documents and evidence set forth in Attachment B.

---

Grayden R. Ridd  
Special Agent  
Federal Bureau of Investigation

Sworn to and subscribed before me  
this 5th day of March 2013.

---

John M. Facciola  
United States Magistrate Judge



## **ATTACHMENT A**

### **Property to Be Searched**

A residential condominium dwelling located at The Watergate, 2700 Virginia Avenue, N.W., #901, Washington, D.C. 20037. The building's external entrance is identified as "Watergate West" in metallic letters, gold in color. Under "Watergate West" appears the number 2700, written in metallic numbers, gold in color. Unit 901 is located on the west end of the building on the 9<sup>th</sup> floor. It is identified by a metallic plaque, gold in color, on which appears the number "901."

## **ATTACHMENT B**

### **Property to be Seized**

Evidence, fruits, instrumentalities and/or proceeds of violations of, and conspiracy to violate, United States laws prohibiting and regulating transactions with the Government of Sudan and its officers and entities, and commercial transactions relating to the Republic of Sudan, in violation of 50 U.S.C. §§1701-1706 (International Emergency Economic Powers Act - IEEPA), 31 C.F.R. Part 538 (Sudanese Sanctions Regulations), whether or not such transactions were actually completed, as well as violations of, and conspiracy to violate, of 18 U.S.C. §951 (Agent of a foreign government), and 18 U.S.C. §371 (Conspiracy).

Such items include, but are not limited to, all records, in any form reflecting or relating to the following:

1. Activities involving Robert C. McFarlane; McFarlane Associates, Inc., and its employees and agents; and any other person or entity, in connection with the Governments of Sudan and Qatar.
2. Financial transactions by or on behalf of Robert C. McFarlane; McFarlane Associates, Inc., and its employees and agents.
3. Knowledge of, and compliance or noncompliance with, United States laws relating to the Government of Sudan or any of its officers or entities.

“Records” includes, but is not limited to, the following:

1) correspondence, facsimile (“fax”) communications, electronic mail (“email”) communications, telephone messages, calendars, internal memoranda, notes from meetings and conversations;

2) records and other items reflecting travel by Robert C. McFarlane and known employees of McFarlane Associates, Inc., and travel to or from Sudan and/or Qatar by any other person, including itineraries, tickets, receipts, lodging records, photographs, maps, souvenirs, and guidebooks;

3) contracts, agreements, quotations, purchase orders, invoices, airway bills, and shipping and import/export documentation;

4) bank records such as statements, check stubs and registers, canceled checks, deposit tickets, debit memos, wire transfer documents, certified check memos, and official cashier's check memos, Letters of Credit, bank drafts, and other records of payment;

5) books of original entry, including but not limited to general ledgers, cash receipts, sales, cash disbursements, purchases, payroll, journals, pension/retirement plans, investments, and financial work papers;

6) passports, passport applications, visas, visa applications;

7) any safe and its contents related to the enumerated offenses;

8) computers and computer-related items (including any records, documents, materials and files maintained on a computer), which includes:

a. Any digital device capable of being used to commit, further or store evidence of the offenses listed above;

b. Any equipment used to facilitate the transmission, creation, display, encoding or storage of digital data, including word processing equipment, modems, docking stations, monitors, printers, plotters, encryption devices and optical scanners;

c. Any magnetic, electronic or optical storage device capable of storing data, such as floppy disks, hard disks, tapes, CD-ROMs, CD-R, CD-RWs, DVDs, optical disks, printer or memory buffers, smart cards, PC cards, memory calculators, electronic dialers, electronic notebooks, cellular telephones and personal digital assistants;

d. Any documentation, operating logs and reference manuals regarding the operation of the digital device or software used in the digital device;

e. Any applications, utility programs, compilers, interpreters and other software used to facilitate direct or indirect communication with the digital device;

f. Any physical keys, encryption devices, dongles and similar physical items that are necessary to gain access to the digital device or data stored on the digital device; and

g. Any passwords, password files, test keys, encryption codes or other information necessary to access the digital device or data stored on the digital device.